1-1-2014

The Dark Cloud of Convenience: How the New HIPAA Omnibus Rules Fail to Protect Electronic Personal Health Information

Joyce L.T. Chang
J.D. Candidate, Loyola Law School, 2015

THE DARK CLOUD OF CONVENIENCE: HOW THE NEW HIPAA OMNIBUS RULES FAIL TO PROTECT ELECTRONIC PERSONAL HEALTH INFORMATION

*JOYCE L.T. CHANG**

The 2013 Omnibus Rules (Rules) update to the Health Insurance Portability and Accountability Act (HIPAA) aims to increase the privacy of patient health information (PHI). Although there are increases in monetary penalty fees, there are still two major areas of weakness. First, the Rules fail to address the role of cloud storage technology. Traditionally, PHI was physically stored on-site at medical offices. However, the trend of outsourcing PHI storage to cloud computing creates a huge risk of privacy breaches as currently there are no federal standards on the security of cloud computing. This failure jeopardizes PHI privacy and leaves the medical community uncertain about security and HIPAA compliance. Second, even with increases in monetary penalties, consumer remedies are still limited since there is no private right of action. This Note explains the background of HIPAA, the need for federal guidance on technology security standards, and how in order for HIPAA to be meaningful, consumers need a private right of action against those who have breached the privacy of PHI.

I. INTRODUCTION

"[T]he status quo [of health care is] 'the worst of two worlds.' The U.S. has 'a regulatory industry that is saddled with laws with so many loopholes that they don't know what they are responsible for, and a public that doesn't believe that their health information is being protected.'"[1]

*J.D. Candidate, Loyola Law School, 2015; M.Ed. George Mason University, 2012; B.S. and B.A., University of California, San Diego, 2010. The author would like to thank her family, friends, and colleagues for their support and encouragement during the production of this Note. She would like to thank Professor Brietta Clark for her valuable feedback, constructive guidance, and her smiling presence on campus that brightens up any classroom. She would like to thank her family and friends for their patience and encouragement. She would like to express her sincerest gratitude to the staff of the *Loyola of Los Angeles Entertainment Law Review* for each person's

With a click of a few buttons, someone can access the medical information of 10,000 patients and sell this information for a mere ten or twenty dollars.[2] Breaches of medical records account for 43% of all privacy breaches in the United States.[3] Even with the presence of credit cards and online markets, medical record breaches outnumber breaches involving banking and finance, the government, and the military.[4] These breaches can lead to medical identity theft where victims experience substantial financial repercussions and have to deal with the long-term effects of erroneous information being added to their medical files.[5] For example, a Pennsylvania man found that an imposter used his identity at five different hospitals to receive more than $100,000 in treatment.[6]

Traditionally, health care providers stored PHI data on-site through the use of desktop computers, internal software programs, and physical memory devices.[7] However, with increasing patient caseloads, medical organizations have turned to cloud technology to address the storage, communication, and analysis of PHI.[8] By outsourcing the technology and maintenance of PHI to third party cloud storage providers,[9] healthcare

---

contribution to this Article, especially editors Scott Salomon, Elena Sadowsky, Seema Ghatnekar, and Jacquelyn Young. Finally, she would like to thank each reader for their interest and time in this Article.

1. *See* Michael Ollove, *The Rise of Medical Identity Theft*, THE PEW CHARITABLE TRUSTS (Feb. 7, 2014, 2:00 PM), http://www.pewstates.org/projects/stateline/headlines/the-rise-of-medical-identity-theft-85899539025 (quoting James Pyles, a Washington D.C. lawyer with forty years of health law experience).

2. *See id.* (quoting Sam Imandoust of the Identity Theft Resource Center).

3. *See id.*

4. *See id.*

5. *See id.*

6. *See id.*

7. Michael Daray, *Negotiating Electronic Health Record Technology Agreement*, 22 HEALTH LAW 53, 54 (2009).

8. Frank Pasquale & Tara Adams Ragone, *The Future of HIPAA in the Cloud*, SETON HALL LAW CENTER FOR HEALTH & PHARMACEUTICAL LAW & POLICY, 3 (June 30, 2013), *available at* http://law.shu.edu/ProgramsCenters/HealthTechIP/HealthCenter/upload/hipaa-in-the-cloud-07012013.pdf.

9. *See* Clay B. Wortham, *Is HIPAA In The Clouds?*, HEALTH CARE LAW (Sept. 17, 2012),

groups can focus on patient care[10] while patient security and privacy can be managed independently.[11] Smaller organizations no longer have to invest in expensive hardware or use employee time to manage information technology infrastructure.[12] Therefore, outsourcing the storage of information allows for a more patient-centered and efficient use of time and resources.[13]

Two hundred years before the existence of cloud technology, Thomas Jefferson warned that in order "to penetrate and dissipate clouds of darkness, the general mind must be strengthened by education."[14] Currently, cloud computing technology offers users the convenience to "take care of everything. And you barely have to do a thing."[15] For example, Apple's iCloud offers users the convenience of accessing the same content on multiple devices.[16] The technology of cloud computing[17]

---

http://mcbrayerhealthcare.com/2012/09/17/is-hipaa-in-the-clouds/ (noting that cloud storage data is beneficial to medical providers since the servers can be at multiple physical locations, unlike traditional onsite data storage); *see generally* Lisa Boch-Anderson, *Hospital Uses Cloud Computing to Improve Patient Care and Reduce Costs*, MICROSOFT EUROPE (Apr. 15, 2011), http://www.microsoft.com/eu/transforming-business/multimedia/hospital-uses-cloud-computing-to-improve-patient-care-and-reduce-costs.aspx (describing the hospital's transition to cloud computing).

10. Wendy Kaufman, *Cloud Computing Saves Health Care Industry Time and Money*, NATIONAL PUBLIC RADIO (Oct. 1, 2012, 2:49 PM), http://www.npr.org/blogs/alltechconsidered/2012/10/01/162080613/cloud-computing-saves-health-care-industry-time-and-money.

11. Mina Deng, Milan Petkovic, Marco Nalin & Ilaria Baroni, *A Home Healthcare System In The Cloud – Addressing Security and Privacy Challenges*, 2011 IEEE INTERNATIONAL CONFERENCE ON CLOUD COMPUTING (CLOUD) Washington, D.C., (July 4–9, 2011) 549–556, http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=6008754.

12. Saurabh Kumar Garg, Steve Versteeg & Rajkumar Buyya, *A Framework for Ranking of Cloud Computing Services*, 29 FUTURE GENERATION COMPUTER SYSTEMS 1012, 1012 (2013).

13. *Id.*

14. Thomas Jefferson, *From Thomas Jefferson to Francois Adriaan Van der Kemp, 9 July 1820*, FOUNDERS ONLINE, NATIONAL ARCHIVES (July 9, 1820), http://founders.archives.gov/documents/Jefferson/98-01-02-1374.

15. *iCloud – All of Your Content on All of Your Devices*, APPLE, http://www.apple.com/icloud/features/ (last visited Apr. 16, 2014, 9:25 AM).

16. *Id.*

17. Chunming Rong, Son T. Nguyen & Martin Gilje Jaatun, *Beyond Lighting: A Survey on Security Challenges in Cloud Computing*, 39 COMPUTERS AND ELECTRICAL ENGINEERING 47, 47 (2013) ("According to Google's Kevin Marks, the term 'cloud computing' comes 'from [the]

and storage[18] has revolutionized commerce for corporations such as Amazon,[19] Dropbox,[20] and Google.[21] As more people[22] and entities[23] rely on the convenience of cloud technology, this convenience creates serious privacy and security concerns[24] about the storage and transmission of PHI.[25] PHI that is created, stored, transmitted, or received electronically

---

early days in the Internet where we drew the network as a cloud. We didn't care where the message went…the cloud hid it from us.'").

18. *See* Arif Mohamed, *A History of Cloud Computing*, COMPUTER WEEKLY (Mar. 2009), http://www.computerweekly.com/feature/A-history-of-cloud-computing (describing the origin and development of the cloud from 1969 when "the idea of an intergalactic computer network was introduced" to current day cloud computing and how IT directors "will need to continue to manage their internal computing environments, whilst learning how to secure, manage, and monitor the growing range of external resources residing in the cloud.").

19. *See Amazon Cloud Drive: Learn More*, AMAZON, http://www.amazon.com/gp/feature.html?docId=1000796931 (last visited Apr. 16, 2014) (describing how Amazon Cloud allows subscribers to protect all digital content, access personal photos and videos anywhere, and receive five free gigabytes of storage with Cloud Drive).

20. *See* Laurel Storm, *How to Use Dropbox for Better Document Management & Team Collaboration*, GLOBAL POST, http://everydaylife.globalpost.com/use-dropbox-better-document-management-team-collaboration-37079.html (last visited Mar. 21, 2014) (describing how Dropbox can be used by companies to facilitate information sharing).

21. *See Google Cloud Storage – A Simple Way to Store, Protect, and Share Data*, GOOGLE, https://cloud.google.com/files/CloudStorage.pdf (last visited Apr. 16, 2014) (describing how corporations and every day users can utilize Google Cloud for collaborative projects from multiple locations).

22. *See* Quentin Hardy, *Box and Dropbox Come of Age in Cloud Computing*, N.Y. TIMES (July 31, 2012, 9:00 AM), *available at* bits.blogs.nytimes.com/2012/07/31/box-and-dropbox-coming-of-age-in-cloud-computing/?_r=0 (quoting Aaron Levie, CEO of Box, discussing how corporations are rapidly outsourcing data storage and how it is "amazing how quickly business are getting behind the idea of not managing their own equipment . . . .").

23. *See id.* (explaining how Amazon was one of the first to offer cloud computing program Simple Storage Service (S3) in 2006. S3 was highly technical and less user-friendly. However, the increase of user friendly interface and improved customer services of cloud computing corporations such as Dropbox have significantly increased cloud computing usage.).

24. Lucas Mearian, *"Wall of Shame" Exposes 21M Medical Record Breaches – Notification, Reporting Part of New Rules under the Health Information Technology for Economic and Clinical Health Act*, COMPUTERWORLD (Aug. 7, 2012, 6:00 AM), http://www.computerworld.com/s/article/9230028/_Wall_of_Shame_exposes_21M_medical_record_breaches?pageNumber=1.

25. *See* 45 C.F.R. § 160.103 (2014) ("[P]rotected health information means individually identifiable health information . . . that is . . . transmitted or maintained in any form or medium . . . Protected health information excludes individually identifiable health information" in certain

through cloud technology is classified as electronic protected health information (ePHI).[26]

Despite these benefits, ePHI has been associated with greater opportunities for identity theft and medical insurance fraud.[27] Additionally, the electronic equipment that houses ePHI is often portable and expensive, creating a potential for theft.[28] The United States Department of Health and Human Services (HHS) estimates that at least half of all medical-related security breaches involve the theft of a computer or other electronic device.[29] For example, the burglary of three laptops from a dental center jeopardized the PHI of 850 patients; however, in that case it was unclear whether the information was compromised or if the thieves were more interested in the laptops.[30]

Even before advances in privacy technology and cloud computing, PHI and ePHI could be breached from simple human error.[31] In 2009, a billing employee at Harvard University's Massachusetts General Hospital was commuting on a Boston subway when she lost a USB[32] containing

---

education records and in employment records held by a covered entity as its role as employers, and also excludes individually identifiable health information regarding person who have been deceased over fifty years from protected health information.).

26. University Information Technology Services, *What is Protected Health Information?*, INDIANA UNIVERSITY (Dec. 11, 2013), http://kb.iu.edu/data/ayyz.html.

27. Michelle S. Huffman, *Electronic Health Records Could Make Medical Identity Theft Easier*, IDENTITY PROTECTION (May 1, 2013, 8:35 PM), http://www.identityprotection.com/education/id-theft-101/-/asset_publisher/oTaWN9aifqCr/content/electronic-health-records-could-make-medical-identity-theft-easier/pop_up?_101_INSTANCE_oTaWN9aifqCr_viewMode=print.

28. *See generally* Ben Sutherly, *Three Stolen Laptops Had Information on Patients*, THE COLUMBUS DISPATCH (Feb. 5, 2013, 7:57 AM), http://www.dispatch.com/content/stories/local/2013/02/05/three-stolen-laptops-had-information-on-patients.html (using laptops as an example of electronic equipment that commonly houses ePHI, but also carries a substantial risk of theft due to portability and high value).

29. Ollove, *supra* note 1.

30. Sutherly, *supra* note 28.

31. HIPAA Security Series, *6 Basics of Risk Analysis and Risk Management*, DEPARTMENT OF HEALTH & HUMAN SERVICES – CENTERS FOR MEDICARE & MEDICAID SERVICES (June, 2005) *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf.

32. *See* Bradley Mitchell, *What Is A USB Port?*, ABOUT.COM COMPUTING WIRELESS/NETWORKING, http://compnetworking.about.com/od/usbnetworking/p/usb-port.htm (last visited Feb. 25, 2014) (explaining that USB stands for Universal Serial Bus and allows users

ePHI of 192 patients.[33] The ePHI contained names, dates of birth, medical records, health insurance policy numbers, and HIV/AIDS status.[34] Massachusetts General Hospital agreed to pay a one million dollar settlement to HHS.[35] Thus, the average privacy breach was settled for a mere $5,000.[36] Furthermore, none of the money went to the patient whose information was breached.[37]

Cloud technology exacerbates privacy risks since there are ambiguous security requirements and the convenience of accessing data on the cloud also increases the opportunities for security breaches.[38] With cloud technology, PHI and ePHI stored in large healthcare agencies are now more susceptible to privacy breaches.[39] Recently, TRICARE Management Activity (the healthcare program of the United States Department of Defense Military Health System) reported 4.9 million records of misplaced ePHI when backup media could not be found.[40] The potentially compromised data included names, Social Security numbers, addresses, diagnoses, treatment information, provider names, provider data, and other

---

to transfer information through a small device called a USB port).

33. Carey Goldberg, *MGH Settles for $1M After HIV Patient Records Lost on Subway*, 90.9 WBUR BOSTON'S NPR NEWS STATION (Feb. 24, 2011, 4:53 PM), http://commonhealth.wbur.org/2011/02/mass-general-privacy/.

34. *Id.*

35. *Id.*

36. *See generally id.*

37. *See id.* (generally describing the incident on the subway and that the $1 million settlement was paid to the U.S. Department of Health and Human Services).

38. Nathan Pearce, *Can Cloud Computing Overcome Its Crisis of Confidence?*, THE GUARDIAN (Feb. 18, 2014, 6:59 AM), http://www.theguardian.com/media-network/media-network-blog/2014/feb/18/cloud-computing-nsa-privacy-breaches-crisis-confidence.

39. *See* Barton Gellman and Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, THE WASHINGTON POST (Oct. 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (describing how even the NSA's use of cloud computing can be exposed to security and privacy breaches).

40. Tricare News, *Risk to Patients from Data Breach Met with Proactive Response*, TRICARE (Nov. 23, 2011), http://www.tricare.mil/Welcome/MediaCenter/News/Archives/58_DataBreach.aspx.

patient information.[41] WellPoint, the largest managed healthcare company in the Blue Cross and Blue Shield Association, also reported that 612,402 customer records were compromised due to inadequate security measures.[42]

To address privacy concerns of PHI, Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[43] The most recent revisions to the HIPAA regulations aim to increase privacy (hereinafter "the Rules"); however, the Rules fail to provide significant proactive enforcement mechanisms and merely increase the population that has to follow the Rules.[44] Additionally, the Rules do not adequately address the entire scope of ePHI.[45] Specifically, the security provisions of the Rules explicitly avoid defining technological requirements for storage of PHI and ePHI.[46] Instead, the Rules specifically take on a "technologically neutral" position so that each organization can determine which technology will meet the organization's needs.[47] While cloud computing offers convenience, it is difficult for medical providers to determine what type of cloud is best for being in compliance under the

---

41. PHIPrivacy, *Tricare Discloses SAIC Breach: Backup Tapes Held Data on 4.9 Million*, PHIPRIVACY.NET (Sept. 29, 2011), http://www.phiprivacy.net/tricare-discloses-saic-breach-backup-tapes-held-data-on-4-9-million/.

42. Jennifer R. Bruer, Sarah H. Shanti, David A. Mayer & Fatema Zani, *WellPoint, Inc. Pays HHS $1.7 Million To Settle Affiliated Covered Entity's Alleged HIPAA Violations*, MONDAQ (Aug. 6, 2013), http://www.mondaq.com/unitedstates/x/256366/Healthcare/WellPoint+Inc+Pays+HHS+17+Million+To+Settle+Affiliated (noting that WellPoint "failed to (1) adequately implement policies and procedures for authorizing access to ePHI in the database; (2) perform an adequate risk analysis following a software upgrade that affected the database; and (3) adequately implement technical safeguards to verify the identity of persons trying to access ePHI in the database.").

43. Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules, 78 Fed. Reg. 5566, 5566 (proposed Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 and 164) [hereinafter *Modifications*] (describing modifications to HIPAA).

44. *See id.* at 5569 (describing modifications to HIPAA).

45. *See id.* (describing modifications to HIPAA).

46. *See* Rong et al., *supra* note 17 (providing examples of technological specifications including network architecture, data format, metering and billing, Quality of Service agreements, resource provisioning, etc.).

47. *Modifications*, *supra* note 43, at 5589.

Rules.[48] Given that most ePHI is stored on some form of cloud technology, the potential for security loopholes greatly impacts consumer privacy.[49]

The lack of standardized technology requirements creates uncertainty as to what it takes to have a HIPAA compliant cloud that protects the privacy of PHI and ePHI.[50] Additionally, there are no standardized measures or public metrics to analyze what constitutes a HIPAA security compliant and effective cloud computing system.[51] In order for covered entities and business associates to remain compliant with the Rules, meet their work demands, and effectively care for patient ePHI, there must be a "way to identify and measure key performance criteria" that are essential to cloud computing.[52]

Additionally, this Note argues that the liability provisions of the Rules do not provide enough privacy protection for individual consumers. Given that the risks of privacy breaches of PHI are exacerbated by cloud technology,[53] the Rules should address the increased risks to compensate consumers. Furthermore, the Rules do not give consumers a private right of action.[54] If a breach occurs, consumers report the breach to the Department of Health and Human Services (HHS).[55] HHS then has the

---

48. Garg et al., *supra* note 12.

49. *See Modifications*, *supra* note 43, at 5589 ("[T]he requirements of the Security Rule were designed to be technology neutral and scalable to all different sizes of covered entities and business associates.").

50. Garg et al., *supra* note 12 (discussing the variation in Cloud offerings).

51. *Id.* (describing that while the technology world has not established a standardized measure of what constitutes a high quality cloud, different factors have been identified as possible measures. These factors include accountability, agility, cost performance, assurance, security and privacy, and usability.).

52. *Id.*

53. Huffman, *supra* note 27.

54. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82566 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160 and 164); *see HIPAA Violations and Enforcements*, AMERICAN MEDICAL ASSOCIATION, http://www.amaassn.org//ama/pub/physician-resources/ solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page (last visited Apr. 16, 2014 at 3:16 PM).

55. *See* Patrick Ouellette, *Will Walgreens Breach Ruling Affect Future HIPAA Violations?*, HEALTHITSECURITY (Aug. 13, 2013), http://healthitsecurity.com/2013/08/13/will-walgreens-breach-ruling-affect-future-hipaa-violations/
(describing how HIPAA violations are typically reported directly to the U.S. Department of

discretion to pursue an investigation to determine the appropriate penalty.[56] Although the Rules increase the amount of monetary fines for privacy breaches, none of the fines go directly to the consumer.[57]

Though the Rules are a step in the right direction, the failure to adequately address the role of technology with PHI and ePHI creates several loopholes in the new era of the Rules and HIPAA. This Note will address and explain why the Rules do not provide enough privacy protection for consumers. The Rules fail to provide explicit technology guidelines on what a secure, HIPAA compliant cloud looks like. Additionally, consumers are not given any private right of action to pursue breaches of PHI. Part II explains the background issues and defines key terminology to establish the foundation necessary to understand the Rules. Part III identifies and analyzes specific changes in the Rules that impact the privacy of patient ePHI. Part III also discusses and synthesizes technology and privacy concerns in the new regime of HIPAA and the Rules. Although the Rules allow federal authorities to impose stricter regulations and harsher penalties, a major deficiency is that the Rules do not allow for private causes of action. Finally, Part IV provides recommendations on how legislators should proceed in the new era of HIPAA.

II. BACKGROUND OF THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

HIPAA established the first set of federal standards to protect the privacy of PHI.[58] However, HIPAA has caused confusion for health care providers, legislatures, and consumers.[59] The misunderstanding of HIPAA

Health and Human Services who then decides whether or not to investigate claims of privacy breach).

56. Kimberly J. Kannensohn, Nathan A. Kottkamp, Vincent A. Dongarra & Amanda L. Enyeart, *HIPAA Omnibus Final Rule Implements Tiered Penalty Structure for HIPAA Violations*, MCGUIREWOODS (February 14, 2013), https://www.mcguirewoods.com/Client-Resources/Alerts/2013/2/HIPAA-Omnibus-Final-Rule-Implements-Tiered-Penalty-Structure-HIPAA-Violations.aspx.

57. *See* Ouellette, *supra* note 55 (quoting HHS Director Leon Rodriguez who explains that HIPAA funds go toward "further enforcement and victim restitution." However, Mr. Rodriguez's answer does not provide transparency about what exactly is done with the fines or what actual programs are available for victims.).

58. SHARYL J. NASS, LAURA A. LEVIT & LAWRENCE O. GOSTIN, BEYOND THE HIPAA PRIVACY RULE: IMPROVING HEALTH THROUGH RESEARCH 1-2 (2009).

59. *See* Jane Gross, *Keeping Patients' Details Private, Even From Kin*, N.Y. TIMES (July

results in inconsistent application of the Rules.[60] The overzealous application of HIPAA prevents family members, caretakers, public health officials, and law enforcement officials from obtaining health information.[61] For example, nurses threatened to evict and arrest a man who was at the bedside of his father-in-law, who was being treated for a stroke.[62] HIPAA also frustrates adult children who are caring for their parents from a distance. Often, healthcare providers refuse to provide information on the rationale that information cannot be shared because of HIPAA.[63]

A. Definitions of Key Terminology in the Rules

For purposes of clarity and consistency, key terminology used in the text of the Rules are described below.

1. Covered Entities

Covered entities include: "a health plan, a health care clearinghouse, and a health care provider who transmits any health information in electronic form in connection with a transaction" covered under Subchapter C of HIPAA.[64] If a covered entity wants to disclose PHI, the patient must authorize the disclosure in writing.[65] The Rules require that covered entities have administrative[66] and physical[67] safeguards that govern how

---

3, 2007), http://www.nytimes.com/2007/07/03/health/policy/03hipaa.html?pagewanted=all&_r=0 (referencing government studies that show frustration with HIPAA is widespread).

60. *Id.*

61. *Id.*

62. *Id.*

63. *Id.*

64. 45 C.F.R. § 160.103 (2014).

65. *See* 45 C.F.R. § 164.502 (2014) (requiring written authorization for disclosure from the patient or the patient's representative).

66. *See* 45 C.F.R. § 164.304 (2014) ("[A]dministrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.").

covered entities maintain their organizational practices and engage with others.[68] Most significantly, covered entities are required to ensure that any outsourced or subcontracted PHI also complies with the Rules.[69]

2. Business Associates

A business associate is defined as a person or entity "that creates, receives, maintains or transmits" PHI on behalf of a covered entity[70] for purposes of a regulated function or activity (e.g. claims processing, data analysis, utilization, quality assurance, and billing),[71] or a person or entity that "provides . . . legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services where the provision of such services involves the disclosure[72] of protected health information."[73] Applying this definition, a business associate includes (1) a Health Information Organization (HIO), E-Prescribing Gateway, or other person that provides data transmission services of PHI to a covered entity and that requires access on a routine basis to such PHI; (2) a person who offers a personal health record to one or more individuals on behalf of a covered entity; and (3) a subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate.[74] Most importantly, and

---

67. *See id.* ("[P]hysical safeguards are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.").

68. *See* 45 C.F.R. § 164.306 (2014) (listing general requirements of security standards, e.g. technical requirements, policies and procedures and documentation requirements, etc.).

69. *See* 45 C.F.R. § 164.314 (2014) (stating the organizational requirement that "any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section . . . .").

70. 45 C.F.R. § 160.103(1)(i) (2014).

71. *Are You a Business Associate Under the HIPAA Privacy and Security Rules*, HEALTH INFO. & THE LAW (Sept. 12, 2013), http://www.healthinfolaw.org/sites/default/files/article-files/Fast%20Facts%20%20-%20Are%20you%20BA.pdf.

72. *See* 45 C.F.R. § 160.103 ("Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.").

73. *Id.*

74. 45 C.F.R. § 160.103(3).

unlike the former rules, the Rules require that business associates must also report security breaches in PHI and ePHI directly to covered entities.[75]

3. Breaches

A breach occurs when the business associate had knowledge or by exercising reasonable diligence would have known that there was a breach in PHI.[76] Breaches are defined as "the acquisition, access, use, or disclosure of [PHI] in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health care information."[77]

The Rules specifically state three scenarios that are excluded from the definition of breach.[78] The first exclusion occurs when PHI is unintentionally accessed by someone acting under the authority of the HIPAA covered entity or business associate.[79] An example of unintentional access would occur when a HIPAA covered entity or business associate employee opened an email mistakenly sent; however, the email is deleted and the sender is immediately notified of the mistake.[80] The second exclusion occurs where there is inadvertent disclosure of PHI.[81] In the email example, the sender of the email would have inadvertently disclosed PHI.[82] The third and final exclusion occurs when there is a "good faith belief" that it would be unreasonable to retain the breached data.[83] An example of unreasonably retained PHI would be a medical report that was incorrectly mailed but returned to the original sender

75. 45 C.F.R. § 164.410(a)(1) (2014).

76. 45 C.F.R. § 164.410(a)(2).

77. 45 C.F.R. § 164.402 .

78. 45 C.F.R. § 164.402(1).

79. 45. C.F.R. § 164.402(1)(i); *see* KATHY BAKICH & KAYE PESTAINA, EMPLOYER'S GUIDE TO HIPAA PRIVACY REQUIREMENTS ¶*570* (2013).

80. *See id.*

81. 45. C.F.R. § 164.402(1)(ii); *see* BAKICH & PESTAINA, *supra* note 79.

82. *See* BAKICH & PESTAINA, *supra* note 79.

83. 45. C.F.R. § 164.402(1)(iii); *see* BAKICH & PESTAINA, *supra* note 79.

unopened and labeled as undeliverable.[84] The unopened envelope would demonstrate that no one actually viewed the PHI.[85]

B. Outside of the Rules: How The Technology of the "Cloud" Casts Its Shadows Over the Rules

Cloud computing[86] is a growing technological industry with an estimated market size of $150 billion by 2014.[87] The National Institute of Standards and Technology defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[88] Although there are an infinite number of user specifications, cloud computing has five essential characteristics.[89]

First, cloud computing has on-demand self-service.[90] The on-demand feature allows consumers to use unilateral provision computing capabilities such as accessing external servers and network storage automatically without human interaction.[91] Second, cloud computing allows for broad network access.[92] Third, cloud computing allows for resource pooling where multiple users can combine their resources and access the collective resources from different locations.[93] For example, Google Docs is a

84. BAKICH & PESTAINA, *supra* note 79.

85. *Id.*

86. *See generally* Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing*, NATIONAL INSTITUTE OF STANDARDS TECHNOLOGY 2 (Sept. 2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

87. Sara Angeles, *8 Reasons to Fear Cloud Computing*, BUSINESSNEWSDAILY, (Oct. 1, 2013, 11:07 AM), http://www.businessnewsdaily.com/5215-dangers-cloud-computing.html.

88. Mell & Grance, *supra* note 86, at 2.

89. *Id.*

90. *Id.*

91. *Id.*

92. *Id.*

93. *Id.*

commonly used resource-pooling tool[94] where users can simultaneously access the same version of a document from different locations.[95] However, the multiple users generally have no control or knowledge of where the exact location of the data storage actually occurs.[96] Fourth, cloud computing has rapid elasticity that allows users to scale the amount of storage they use based on their needs.[97] Finally, cloud computing provides users measured services.[98] These services allow for the optimization of resource use within the cloud system based on the storage, processing, and bandwidth utility and capability within that system.[99]

The lack of compliance and standards among cloud computing is stunting the pace of technological growth for cloud computing.[100] Not all clouds are created equally, and each organization should analyze their business needs, customer expectations, and compliance with the Rules before committing to a certain type of cloud computing provider.[101]

Cloud computing can be implemented in a variety of formats.[102] The most relevant types of clouds are private clouds,[103] hybrid clouds,[104] and

---

94. *See generally* Google, *Docs, Sheets, and Slides*, GOOGLE, https://support.google.com/drive/answer/49008?hl=en (last visited Apr. 16, 2014 at 4:13 PM) (describing how Google Docs functions).

95. *Id.*

96. Mell & Grance, *supra* note 86, at 2.

97. *Id.*

98. *Id.*

99. *Id.*

100. *See* Haralambos Mouratidis, Shareeful Islam, Christos Kalloniatis & Stefanos Gritzalis, *A Framework to Support Selection of Cloud Providers Based on Security and Privacy Requirements*, 86 THE J. OF SYSTEMS & SOFTWARE 2276, 2277 (2013).

101. *See generally id.*

102. *See* Mell & Grance, *supra* note 86, at 2-3.

103. *See id.* at 3 (describing how private cloud is a "cloud infrastructure [which] is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.").

104. *See id.* (describing how hybrid cloud is a "cloud infrastructure . . . composition of

community clouds.[105] Private clouds are generally considered safer than other clouds since usage is limited to a single customer.[106] Thus, private clouds are infrastructure dedicated solely to the needs of a particular organization and are not shared with any other organizations.[107]

In contrast, public clouds are usually owned by large organizations and involve multiple users.[108] Generally, most people are familiar with public clouds such as Amazon, Microsoft, and Google.[109] A major concern in public clouds or cloud computing systems with multiple users is data segregation.[110] Multiple consumers' data is stored in the same cloud and must be separated based on who is accessing the cloud.[111] For example, a 2009 security flaw in Google Docs exposed personal documents to other Google Doc users.[112] Additionally, customers who use public clouds are

---

two or more distinct cloud infrastructures (private, community, or public) that remains unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).").

105. *See id.* (describing how community cloud is an "infrastructure [which] is provisioned for the exclusive use by a specific community of consumers from organizations that have shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.").

106. Mouratidis et al., *supra* note 100, at 2277 (describing that, "[d]ue to this exclusiveness, a private cloud is considered safer than the other models.").

107. *See* Josh Ames, *Types of Cloud Computing: Private, Public, and Hybrid Clouds*, THE APPCORE BLOG (Dec. 12, 2012, 9:16 AM), http://blog.appcore.com/blog/bid/167543/Types-of-Cloud-Computing-Private-Public-and-Hybrid-Clouds (describing how there are two variations of private clouds. First, on-premise private clouds are a type of cloud "hosted within an organizations own facility . . . and are best used for applications that require complete control and configurability of the infrastructure and security. Second, externally hosted private clouds are "also exclusively used by one organization, but are hosted by a third party specializing in cloud infrastructure. The service provider facilitates an exclusive cloud environment with full guarantee of privacy. This format is recommended for organizations that prefer not to use a public cloud infrastructure due to the risks associated with the sharing of physical resources.").

108. *Id.* (describing that, "Public clouds require much more investment compared to private cloud and usually owned by large organisation. In a public cloud, security issues are more critical due to aspects such as virtualisation, which arise from supporting multiple users. Security measures, such as ensuring access control, data access, and availability of individual customer resources is necessary for a secure multi-tenant environment. In case of a hybrid cloud . . . .").

109. *Id.*

110. Mouratidis et al., *supra* note 100, at 2277.

111. *Id.*

not given control of where their PHI is stored in the cloud infrastructure and have limited ability to configure their security preferences.[113]

Hybrid clouds are a combination of two unique clouds that are bound together to maximize the efficiency of a cloud.[114] For example, spreading data to off-site and on-site clouds can allow data storage to occur wherever is most efficient.[115] Community clouds involve an infrastructure that is shared with multiple users and is managed and secured by a third-party-managed service provider.[116] Typically, community clouds are used by private hospitals or groups of clinics.[117]

Rather than investing substantial money in archiving medical records within the hospital, many hospitals are relying on cloud computing storage to address their storage needs.[118] Cloud computing allows multiple users to use their desktop computers, tablets, or smartphones to simultaneously access data that is stored on remote servers.[119] Currently, an estimated fifteen percent of health care providers in the United States use cloud-based storage for images.[120] Experts estimate that within the next three years, more than half of all health systems will switch to using cloud storage for medical imaging.[121]

Cloud computing is not just a form of information outsourcing.[122] To

---

112. *Id.*

113. *See* Ames, *supra* note 107.

114. *See id.* (providing further descriptions of hybrid cloud computing and its uses).

115. *Id.*

116. *Id.*

117. *Id.*

118. *See* Laura Landro, *Where Do You Keep All Those Images?*, WALL ST. J. (Apr. 8, 2013, 4:00 PM), http://online.wsj.com/article/SB10001424127887323419104578374420820705296.html (explaining how cardiology department in Detroit had more than 25,000 patient heart images produced each year. Rather than invest almost $200,000 in new hardware and software upgrades, hospital chose to use cloud computing as a more affordable solution.).

119. *Id.*

120. *Id.*

121. *Id.*

122. Frank Pasquale & Tara Adams Ragone, *The Future of HIPAA in the Cloud*, SETON

meet the growing demands of the medical field, medical schools are incorporating technology into their curricula and skills training for medical students.[123] For example, a partnership with Apple provided all incoming medical students at the University of California, Irvine, with iPads.[124] These iPads were equipped with digital stethoscope and diagnostic ultrasound applications that can digitally record and transmit encrypted PHI.[125]

Third party service providers operate most cloud computing services.[126] These third party service providers handle everything from performing software updates to managing security breaches.[127] Although the third party service providers have a financial incentive to protect ePHI, the incentive is not as high as the medical provider's or the consumer's own incentive to protect his or her own PHI.[128]

HHS has identified three major categories of external privacy breaches caused by remote access programs like the cloud – access, storage, and transmission.[129] Furthermore, internal cyber-attacks and security breaches are a growing concern for cloud computing providers.[130] Edward Snowden's leak of NSA surveillance information is an example of

---

HALL LAW CENTER FOR HEALTH & PHARMACEUTICAL LAW & POLICY, 6 (June 30, 2013), *available at* http://law.shu.edu/ProgramsCenters/HealthTechIP/HealthCenter/upload/hipaa-in-the-cloud-07012013.pdf.

123. *See UCI's iMedEd Initiative named a 2012 – 13 Apple Distinguished Program*, UCIRVINE NEWS (Feb. 11, 2013), http://news.uci.edu/press-releases/ucis-imeded-initiative-named-a-2012-13-apple-distinguished-program/ (describing UCI's adoption of iPads for medical students).

124. *Id.*

125. *Id.*

126. Pasquale & Ragone, *supra* note 122, at 3.

127. Angeles, *supra* note 87.

128. *See id.* (quoting Steve Santorelli, former Scotland Yard detective, who states, "No business is ever going to be as rabid about looking after your data as you would or should be. They are in the business of making money from you, after all. Securing your data sometimes becomes a marketing mantra more than a way of life.").

129. *See HIPAA Security Guidance*, DEP'T OF HEALTH & HUM. SERVICES (Dec. 28, 2006), http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf.

130. Angeles, *supra* note 87.

the risk of internal breaches.[131] Thus, the convenience of cloud computing also increases the ease of cyber-attacks.[132] The risk is exacerbated since there is typically a large volume of PHI stored on one cloud.[133] Therefore, cloud storage has the risks involved with PHI privacy breaches and security breaches that can occur with ordinary Internet use, storage, and transmission.[134]

Given the increasing use of technology in PHI management,[135] there is an even greater need for explicit regulations that clearly address privacy and security risks associated with the convenience of technology.[136] For example, many doctors are now attempting to use Skype conference calls for appointments that do not require a physical examination.[137] However, Skype calls are typically not encrypted.[138] Furthermore, the security concerns involved with cloud storage create several risks for both users and providers of cloud storage.[139] Data transferred between users and providers

---

131. Laura Poitras & Glenn Greenwald, *NSA whistleblower Edward Snowden: "I don't want to live in a society that does these sort of things – video"*, THE GUARDIAN (June 9, 2013), http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video.

132. Angeles, *supra* note 87.

133. *Id.*

134. *See* S. Subashini and V. Kavitha, *A Survey on Security Issues in Service Delivery Models of Cloud Computing*, 34 J. OF NETWORK & COMPUTER APPLICATIONS 2 (July 2011).

135. *See* Joseph Kvedar, *A Physician Faces Disciplinary Actions for Seeing Patients on Skype – Early Guidelines for Patient Video Visits*, THE HEALTH CARE BLOG (Sept. 21, 2013), http://www.thehealthcareblog.com/blog/2013/09/21/a-physician-faces-disciplinary-action-for-seeing-patients-on-skype-early-guidelines-for-patient-video-visits/ (stating that state regulations vary from state to state. However, in some states, doctors are permitted to use video technology to conduct appointments. Skype states that its technology is encrypted which theoretically provides that no one would be able to intercept and eavesdrop on a Skype conference call with a doctor. Further research on the safety and privacy of Skype or FaceTime calls is needed.).

136. *See Creating Healthcare Data Applications to Promote HIPAA and HITECH Compliance*, AMAZON WEB SERVICES (Aug. 2012), http://d36cz9buwru1tt.cloudfront.net/AWS_HIPAA_Whitepaper_Final.pdf.

137. *See* Kvedar, *supra* note 135.

138. *Id.*

139. The Rockefeller University, *Dangers of Cloud Storage*, THE ROCKEFELLER INSTITUTE (2013), http://it.rockefeller.edu/index.php?page=about.cloud.storage.

may not be encrypted.[140] Additionally, the hardware on which the data is stored may not be encrypted.[141] Recent studies[142] have also shown that information stored in older devices is recoverable by looking at the device's metadata – an informational blueprint left on SD cards found in old cellular phones.[143] Even with HIPAA compliant servers, it is difficult for ePHI to remain completely confidential.[144] This risk is exacerbated by work models, which allow employees to bring-your-own-device (BYOD)[145] in order to sync different devices and work from multiple locations.[146] The mixing of corporate and personal work data is a problem created by the BYOD trend.[147]

C. Specific Patient Privacy Rules

The two specific rules related to patient privacy of PHI are the HIPAA Privacy Rule[148] (Privacy Rule) and the HIPAA Security Rule[149] (Security Rule).

---

140. *Id.*

141. *Id.*

142. *See generally* George Grispos, William B. Glisson, & Tim Storer, *Using Smartphones as a Proxy for Forensic Evidence contained in Cloud Storage Services*, UNIVERSITY OF GLASGOW (2013), http://arxiv.org/ftp/arxiv/papers/1303/1303.4078.pdf (describing a study).

143. Antone Gonsalves, *Data leakage risks rises with cloud storage services*, CSO ONLINE (Mar. 27, 2013, 8:00 AM), http://www.csoonline.com/article/730853/data-leakage-risk-rises-with-cloud-storage-services.

144. *See id.* ("'[F]rom a forensics perspective there is little you can do on a device today without leaving some kind of remnants,' said Paul Henry, a forensic analyst for Lumension. 'With DropBox, I can typically decrypt the database and get details of your activities and yes you may find actual cached copies of files in memory as well.'").

145. *See* Michael Fitzgerald, *Avoiding basic BYOD blunders*, CSO ONLINE (Feb. 14, 2013), http://www.csoonline.com/article/728841/avoiding-basic-byod-blunders.

146. Gonsalves, *supra* note 143.

147. *Id.*

148. *See generally* 45 C.F.R. § 160.103 (2014).

149. *See generally* 45 C.F.R. §§ 160, 164 (2014).

1. The Privacy Rule

The purpose[150] of the Privacy Rule is to establish a minimum federal standard for protecting PHI while allowing information to flow and promote high quality health care.[151] When enacted, the Privacy Rule established detailed regulations for how PHI can be used and disclosed by covered entities.[152] Disclosure of any PHI includes the release, transfer, provision of access to, or divulging PHI in any matter outside of the entity holding the information.[153]

2. The Security Rule

The goals of the Security Rule[154] are to ensure that (1) only authorized individuals see stored data; (2) individuals only see the data when they need to use it for an authorized purpose; and (3) the data that authorized individuals see is accurate.[155] When the Security Rule was first enacted, the national standards of protection only applied to covered

---

150. *See Health Information Privacy – The Privacy Rule*, DEP'T OF HEALTH & HUM. SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/ (last visited Apr. 19, 2014) ("The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patient's rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.").

151. Nass et al., *supra* note 58, at 2.

152. *See* 45 C.F.R. § 160.103.

153. *See id.*

154. *See* 45 C.F.R. §§ 160, 164.

155. *See* Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules, 78 Fed. Reg. 5566, 5566 (proposed Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 and 164) ("A major goal of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care . . . . The Security rule also promotes the two additional goals of maintaining the integrity and availability of e-PHI.").

entities.[156] As a result, the initial iteration of HIPAA had several loopholes.[157]

First, covered entities are only a small fraction of the population with access to PHI.[158] With increased patient caseloads and improvements in technology, many covered entities would hire business associates to help with the storage and management of PHI.[159] Additionally, researchers who relied on PHI to conduct health research were not considered covered entities and did not have to implement security requirements outlined in the Security Rule.[160] Federal research regulations included protections of privacy; however, there was no specific law that required researchers to implement security protections for research data involving PHI.[161] In contrast, the former Security Rule only protected electronic medical health records and did not require covered entities to implement any security protections for PHI stored in paper format.[162] While technology allows for data to be stored electronically, many health records still only exist in paper form.[163]

III. THE (NEW) RULES

The Rules became effective on March 26, 2013.[164] Covered entities

156. *See id.*

157. *See, e.g.*, Patrick Ouellette, *Compromising Patient Data*, HEALTHITSECURITY (June 7, 2013), http://healthitsecurity.com/2013/06/07/states-compromise-patient-data-privacy-with-research-sales/ (discussing some of HIPAA's loopholes).

158. *See generally* Nass et al., *supra* note 58 (describing numerous groups that can access to PHI for research and public health reasons and explaining how researchers are not covered by HIPAA).

159. Nass et al., *supra* note 58, at 94 (describing the ongoing effort to transition from paper records to help with storage and management of PHI and explaining how the "security of data will continue to grow in importance as the health care industry moves toward greater implementation of electronic health records . . . ").

160. Nass et al., *supra* note 58, at 94.

161. *Id.*

162. *Id.* at 94-97.

163. *Id.* at 100.

164. *See* Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules, 78 Fed. Reg. 5566, 5566 (proposed Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 and 164) [hereinafter Modifications].

and business associates had until September 23, 2013 to become compliant with the Rules.[165] Business associate agreements (BAA) that were entered into before January 25, 2013 were still deemed compliant with the new Rules until the earlier of the date the BAA is renewed, or after September 23, 2013.[166] Most significantly, the Rules included a provision that mandated the Privacy Rule would now apply to business associates who handle PHI for a covered entity.[167] The Rules explicitly state that liability extends down the chain of information technology to include covered entities, business associates, and subcontractors.[168]

Additionally, the Rules now hold that business associates are responsible for complying with all facets of HIPAA's Security Rule.[169] The Rules modified the definition of business associates to explicitly increase the population responsible for complying with HIPAA.[170] Business associates now include health information organizations and any "other person that provides data transmission services with respect to protected health information . . . and that requires access on a routine basis to such protected health information."[171] However, HHS did not define what type of organization would qualify as a health information organization.[172]

The Rules include four significant changes – breach notifications,[173] modifications to the Health Information Technology for Economic and Clinical Health Act (HITECH),[174] changes in the Genetic Information Nondiscrimination Act (GINA),[175] and increases in the amount of civil

165. *Id.* at 5702.

166. *Id.* at 5569, 5702.

167. *Id.* at 5566.

168. *Id.* at 5568.

169. *See* Howard Anderson, *The Security Highlight of HIPAA Omnibus – Shining a Spotlight on Business Associates*, BANK INFO SECURITY (Mar. 1, 2013), http://www.bankinfosecurity.com/blogs/security-highlight-hipaa-omnibus-p-1431.

170. *See* 45 C.F.R. § 160.103 (2014).

171. *Id*.

172. *Modifications*, *supra* note 164, at 5571.

173. 45 C.F.R. §§ 164.402, 164.404 (2014).

174. *Modifications*, *supra* note 164, at 5568.

175. *Id.*

monetary penalties for privacy breaches.[176]

A. Breach Notifications

First, the Rules alter the standards for breach notification of unsecured PHI.[177] Prior to the Rules, only breaches that were a significant risk of privacy violations had to be reported to HHS.[178] Now, when a breach occurs, the presumption is that the information has been compromised.[179] The person or entity responsible for the breach now has the burden of proving that the breach has a low probability of risk.[180]

In order to overcome this presumption and demonstrate there is a low risk that PHI has been compromised, a minimum of four factors are analyzed in the risk assessment.[181] The first factor analyzes the nature of PHI and whether or not there are specific identifiers that would allow for re-identification.[182] Second, a situational analysis is done to see who was authorized to use the PHI and to whom the unauthorized disclosure was made to.[183] The third step looks to see if the PHI was actually viewed by someone else.[184] Finally, the fourth step of the analysis looks to see what steps have been taken to mitigate current and future privacy risks.[185]

---

176. *See* Jane Hyatt Thorpe et al., *Summary and Analysis of the Final Omnibus HIPAA Rule*, GEO. WASH. UNIV. DEP'T OF HEALTH POL'Y 76 (Feb. 13, 2013).

177. Breach Notification for Unsecured Protected Health Information; Interim Final Rule with Requests for Comments, 74 Fed. Reg. 42740 (Aug. 24, 2009) (to be codified at 45 C.F.R. pt 160 and pt. 164).

178. Elizabeth Johnson, *A Comprehensive Summary of the Final Omnibus HIPAA/HITECH Rules: Key Provisions and What They Mean for You*, PONYERSPRUILL 4, http://www.poynerspruill.com/publications/Documents/Summary%20of%20New%20HIPAA%20Rules%20by%20Elizabeth%20Johnson%20Jan%202013.pdf (last visited April 6, 2014).

179. *See* 45 C.F.R. § 164.402(2) (2014).

180. *Id.*

181. *See* 45 C.F.R. § 164.402(2)(i)-(iv).

182. *See* 45 C.F.R. § 164.402(2)(i).

183. *See* 45 C.F.R. § 164.402(2)(ii).

184. *See* 45 C.F.R. § 164.402(2)(iii).

185. *See* 45 C.F.R. § 164.402(2)(iv).

B. Modifications to the Rules Based on the Health Information Technology for Economic and Clinical Health (HITECH) Act

The next significant change of the Rules includes modifications to HITECH's Privacy, Security, and Enforcement Rules.[186] A major modification of the Rules is that business associates are now subject to the Rules.[187] This modification significantly expands the scope of those subject to HIPAA to include any person "who creates, receives, *maintains*, or transmits data on behalf of a covered entity or transmits data on behalf of a covered entity."[188] Based on the wording of the Rules, cloud computing and storage providers are subject to HIPAA because they are managing the exchange of PHI through networks on behalf of covered entities.[189] Even if cloud computing providers do not actually view the PHI, the act of maintaining PHI qualifies them as business associates subject to the Rules.[190] Thus under the new Rules, a covered entity cannot escape liability for their business associates' breaches since business associates are held to the same standards.[191]

A rare exception is granted by the Rules for entities that only provide transmission services of PHI.[192] This exception is designed to exclude couriers[193] who are delivering PHI through mail, on a random or infrequent basis, or as required by other law.[194] The exception also extends to Internet service providers (ISP) who are simply transmitting data.[195]

Most notably under the Rules, the individual consumer does not have

---

186. *Modifications*, *supra* note 164, at 5568-69.

187. *Id.* at 5566.

188. *Id.* at 5572.

189. *Id.*

190. *Id.*

191. *Id.*

192. *See Modifications*, *supra* note 164, at 5571.

193. *Id.* (examples of couriers include the U.S Postal Service and United Parcel Services).

194. *Id.*

195. *Id.*

a private right of action under HIPAA.[196] All HIPAA privacy and security violations must be reported to HHS who then decides whether or not to investigate the charges.[197] Federal agencies are given wide discretion[198] in their decision to charge (or not charge) health care providers with sanctions for privacy breaches of PHI.[199]

C. Monetary Changes Under the Rules: Increased Civil Monetary Penalties and More "Freedom" for Cash Paying Customers

The Rules increase the scope of enforcement and civil monetary penalties for HIPAA violations.[200] Prior to the Rules, civil penalties for unknown and reasonable cause violations could not be more than $100 and the annual maximum fine per calendar year could not exceed $25,000.[201] In contrast, a 2013 survey on medical identity theft shows that victims of medical identity theft paid an average of $18,860 to cover costs associated with privacy breaches.[202]

Categories of Violations and Penalty Amounts
Minimum Penalties per Calendar Year[203]

196. Patrick Oullette, *Will Walgreens Breach Ruling Affect Future HIPAA Violations?*, HEALTHITSECURITY (Aug. 13, 2013), http://healthitsecurity.com/2013/08/13/will-walgreens-breach-ruling-affect-future-hipaa-violations/ (HIPAA violations are typically reported directly to the U.S. Department of Health and Human Services who then decides whether or not to investigate claims of privacy breach).

197. *Id.*

198. *See* Federal Torts Claim Act 28 U.S.C. § 1346(b) (2012) (showing an example of how tort claims against federal entities differ from tort claims against private entities).

199. *See* Oullette, *supra* note 196 (the U.S. Department of Health and Human Services decides whether or not to investigate claims of privacy breach).

200. *Modifications*, *supra* note 164, at 5582.

201. *Id.*

202. Ellen Messmer, *Largely a Family Affair, Medical Identity Theft on the Rise*, NETWORK WORLD (Sept. 12, 2013, 2:36 PM), http://www.networkworld.com/article/2169904/malware-cybercrime/largely-a-family-affair--medical-identity-theft-on-the-rise.html.

203. 42 U.S.C. § 1320d-5 (2012). *See generally*, American Medical Association, *HIPAA Violations and Enforcement*, AMERICAN MEDICAL ASSOCIATION, http://www.ama-assn.org//ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-

Category of Violation[204]	**Former Minimum Penalties**[205]	**New minimum penalties per violation**
Did not know	$100/violation $25,000/repeat violation	$100 - $50,000
Reasonable Cause	$100/violation $25,000/repeat violation	$1,000 - $5,000
Willful neglect – corrected	$10,000/violation $250,000 annual maximum for repeat violations	$10,000 - $50,000
Willful neglect – not corrected	$50,000/violation $1.5 million annual maximum	$50,000

Categories of Violations and Penalty Amounts
Maximum Penalties per Calendar Year[206]

Category of Violation[207]	**Former Maximum Penalty**	**New maximum penalty**

insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page (last visited March 5, 2014 at 7:16 PM).

204. 42 U.S.C. § 1320d-5.

205. *See* Thu Pham, *HIPAA Violation Penalties Rise in Response to Data Breaches*, SMART DATA COLLECTIVE, (Jan. 27, 2013), http://smartdatacollective.com/onlinetech/99671/final-omnibus-rule-raises-hipaa-violation-penalties.

206. 42 U.S.C. § 1320d-5; s*ee generally*, American Medical Association, *HIPAA Violations and Enforcement*, AMERICAN MEDICAL ASSOCIATION, http://www.ama-assn.org//ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page (last visited March 5, 2014 at 7:16 PM).

207. 42 U.S.C. § 1320d-5.

Did not know	$50,000/violation $1.5 million annual maximum	$1.5 million
Reasonable Cause	$50,000/violation $1.5 million annual maximum	$1.5 million
Willful neglect – corrected	$50,000/violation $1.5 million annual maximum	$1.5 million
Willful neglect – not corrected	$50,000/violation $1.5 million annual maximum	$1.5 million

However, it is important to note that the increases are for the *maximum* penalty amount only.[208] HHS specifically states that the maximum penalty will not be imposed in all cases and that the actual penalty amount will be determined on a case-by-case basis.[209] Final penalties are a fact-specific inquiry and include factors such as the time period when the violations occurred and the number of individuals affected.[210] Additionally, the Rules allow covered entities and business associates to establish affirmative defenses by correcting violations within thirty days of having knowledge of any privacy violations.[211]

Under the Rules, cash paying customers can instruct their health care providers not to share information with their health plans.[212] Initially, this seems to benefit the wealthy, who can afford to make cash payments and keep their PHI away from insurance companies who could use the information for insurance underwriting purposes.[213] However, it is

208. *See generally Modifications*, *supra* note 164, at 5583.

209. *Id.*

210. *Id.*

211. *Id.*.

212. Press Release, U.S. Dep't of Health & Human Services, *New Rule Protects Patient Privacy, Secures Health Information* (Jan. 17, 2013), *available at* http://www.hhs.gov/news/press/2013pres/01/20130117b.html.

213. *See generally* Chad Terhune, *Many Hospitals, Doctors Offer Cash Discounts for Medical Bills*, L.A. TIMES (March 27, 2012, 1:17 PM) http://www.latimes.com/business/healthcare/la-fi-medical-prices-20120527,1,676127.story#axzz2rF1ukCr9 (stating that hospitals offer significant discounts for

important to note that the covered entities are still required to disclose PHI, if required by law, even if a customer pays for all of their services in cash.[214]

D. How the Rules Affect Every Day Life

Although the new Rules attempt to empower patients, large corporations still have the ability to bypass certain HIPAA requirements. Starting in February 2013, CVS Caremark encouraged consumers to enroll in the prescription drug rewards program.[215] By enrolling in the rewards program, pharmacy customers can earn up to $50 a year in CVS store credit.[216] Although participation in the rewards program is voluntary, closer examination shows that customers must sign a HIPAA Authorization[217] with alarming consequences for the privacy of customer PHI.

The rationale behind requiring customers to sign a HIPAA Authorization is questionable. When asked why such an authorization was required, CVS spokesman Mike DeAngelis explained, "[CVS] has

---

cash paying customers, even those with insurance. Customers cannot use or notify their insurance company in order to receive the discount. Many insurance companies have pre-negotiated and higher charges).

214. *Modifications*, *supra* note 164, at 5629. ("Under the Privacy Rule, "required by law" is defined at §164.103 as a mandate contained in law that compels a covered entity to make a use or disclosure of PHI that is enforceable in a court of law…this includes Medicare conditions of participation with respect to health providers participating in the program, and statutes and regulations that require the production of information if payment is sought under a government program providing public benefits.").

215. David Lazarus, *CVS Thinks $50 Is Enough Reward for Giving Up Healthcare Privacy*, L.A. TIMES (Aug. 25, 2013, 5:54 PM), www.latimes.com/business/la-fi-lazarus-20130816,5,6795096,full.column#axzz2sgKSjlpA.

216. *Id.*

217. CVS PHARMACY, https://www.cvs.com/extracare/popups/hr_printPopup.jsp?c=false 1/1 (last visited Apr. 16, 2014) ("I hereby authorize CVS/pharmacy® and its affiliates to share my prescription and other health service records, including my email address, with the ExtraCare® program to enroll me in and administer the ExtraCare Pharmacy & Health RewardsTM program, and to inform me of new programs I may be interested in. I understand that (1) my treatment, payment for treatment and eligibility for benefits does not depend on my signing this authorization; (2) after I sign this Authorization, some of my health information as described above, will become part of my ExtraCare Pharmacy & Health Rewards program record and thus no longer covered by the Federal Privacy Rule, but still protected under other consumer protection laws and CVS policy to not share such information outside CVS; (3) I have the right to cancel this authorization at any time . . . Unless I cancel it before then, this authorization will expire one (1) year from today.").

extensive procedures, stringent policies and state-of-the-art technology in place to protect our customers' personal and health information. We do not sell, rent, or give personal information to any non-affiliated third parties."[218] However, by requiring customers to sign such an authorization, CVS is bypassing all the federal requirements of HIPAA.[219] No clarification was provided about what CVS means when the authorization allows for "consumer's health information [to be] potentially re-disclosed."[220] Without the protections of HIPAA, customers participating in the CVS rewards program are no longer protected by federal privacy rules. Instead, consumer privacy laws protect customers where protection levels may vary from state to state.[221] Interestingly, competing pharmacies offer better reward programs without requiring their customers to sign HIPAA Authorizations.[222] Rite-Aid's wellness+ card[223] and Walgreens Balance Rewards Program both offer points every time a prescription is filled, which can be redeemed for cash discounts on store purchases.[224]

In addition to privacy risks, technological difficulties and mismanagement of PHI storage creates huge risks during times of emergencies.[225] For example, a poor network connection[226] could cause

---

218. Patrick Oullette, *CVS Rewards Pprogram Requires Customers to Waive HIPAA Rights*, HEALTH IT SECURITY (Aug. 19, 2013), healthitsecurity.com/2013/08/19/cvs-rewards-program-requires-customers-to-waive-hipaa-rights/.

219. Lazarus, *supra* note 215.

220. *Id.*

221. *See generally* Carolyn L. Carter, *Consumer Protection in the States – A 50-State Report on Unfair and Deceptive Acts and Practice Statutes*, NATIONAL CONSUMER LAW CENTER (Feb. 2009), http://www.nclc.org/images/pdf/car_sales/UDAP_Report_Feb09.pdf.

222. Lazarus, *supra* note 215.

223. *wellness+ Terms & Conditions*, RITE AID, https://www.riteaid.com/wellness/limitation-details (last visited March 5, 2014).

224. *Balance Rewards*, WALGREENS, http://www.walgreens.com/balancerewards/balance-rewards.jsp (last visited April 6, 2014).

225. Jonathon S. Feit, *Why Badly Designed iPad Apps Put Patients at Risk: EMS and ePCR*, THE HEALTH CARE BLOG (Oct. 8, 2013), http://thehealthcareblog.com/blog/2013/10/08/why-badly-designed-ipad-apps-put-patients-at-risk/.

226. Verizon Wireless, *Coverage Locator*, VERIZON WIRELESS, http://www.verizonwireless.com/b2c/support/coverage-locator (last visited Feb. 9, 2014) (showing the limitations of wireless cell phone and Internet coverage in rural and remote locations).

health care providers to lose access to essential ePHI or prevent them from transmitting information to other providers.[227] Additionally, there are compatibility issues that could prevent PHI from being integrated on different devices.[228]

IV. THE NEW ERA: RECOMMENDATIONS FOR IMPROVING PATIENT PRIVACY

Although the Rules allow for federal authorities to impose harsher penalties and stricter privacy requirements, a major gap in privacy protection exists because the Rules do not allow for individual to have private causes of action.[229] The failure to provide a cause of action significantly diminishes the Rules' deterrence effect and potential remedial powers for consumers with breached PHI.[230] Traditionally victims of data breaches and their respective lawyers have interpreted that HIPAA "does not allow for victims to take a covered entity for a private cause of action" and thus cannot sue the source of the breach as individuals.[231]

A. Private Rights of Action and Direct Compensation to Consumers

In a groundbreaking case, an Oregon jury awarded a woman $1.44 million in damages after finding that a Walgreens pharmacist violated her

---

227. Feit, *supra* note 225; *see also*, Chris Gayomali, *Why Apple Is Making an Expensive 128GB iPad*, THE WEEK (Jan. 29, 2013), http://theweek.com/article/index/239380/why-apple-is-making-an-expensive-128gb-ipad (explaining why iPad technology is helpful for consuming content but not helpful in facilitating creation of content. "The iPad shifts the emphasis from creating content to merely absorbing and manipulating it. It mutes you, turns you back into a passive consumer of other people's masterpieces. In that sense, it's a step backward. Not much of a fairy-tale ending. Except for the people who are selling content.").

228. Feit, *supra* note 225.

229. Josh Crank, *Walgreens Sued for Sharing Patient's Private Medical Info*, LAWYERS.COM (Aug. 12, 2013), http://blogs.lawyers.com/2013/08/salgreens-shared-medical-record/.

230. Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 354 – 359 (2007).

231. Patrick Oullette, *Will Walgreens Breach Ruling Affect Future HIPAA Violations?*, HEALTHITSECURITY (Aug. 13, 2013), http://healthitsecurity.com/2013/08/13/will-walgreens-breach-ruling-affect-future-hipaa-violations/.

privacy rights.[232] Walgreens pharmacist Audra Peterson inappropriately accessed Walgreens' customer Abigail Hinchy's prescription data.[233] Abigail was the ex-girlfriend of Audra's current husband, David Peterson.[234] With Abigail's illegally obtained PHI, Audra was able to confirm David's suspicion that Abigail was the source of David's sexually transmitted diseases.[235] David then texted Abigail and told her that he had seen her PHI.[236]

Contrary to typical procedure for reporting HIPAA violations,[237] Abigail called Walgreens directly and informed them of the privacy breach.[238] Despite Abigail's notification, Audra was still able to access Abigail's data for a second time.[239] When questioned about Audra's ability to continue accessing Abigail's data, Walgreens responded that, "[i]t is a misapplication of the law to hold an employer liable for the actions of one employee who knowingly violates company policy."[240] Presiding Judge David J. Dreyer held that while Audra's "subjective motivation could be interpreted as separate from any authorized actions, the nature of her conduct involved training and duties that derived from employment at Walgreens."[241] Although HHS has traditionally governed HIPAA,[242] Judge

---

232. Tim Evans, *Walgreens Must Pay Woman $1.44 Million Over HIPAA Violation*, INDYSTAR.COM (July 26, 2013, 9:26 PM), http://www.indystar.com/article/20130726/NEWS/307260079/Walgreens-must-pay-woman-1-44-million-over-HIPAA-violation?nclick_check=1.

233. Patrick Oullette, *Walgreens Fined $1.44 Million for Ppharmacist Data Breach*, HEALTHITSECURITY (July 29, 2013), http://healthitsecurity.com/2013/07/29/walgreens-fined-1-44-million-for-pharmacist-data-breach/.

234. *Id.*

235. Andrew Scurria, *Walgreen Pharmacy Customer Scores $1.4M Privacy Verdict*, LAW 360 (July 29, 2013, 7:08 PM), http://www.law360.com/articles/460788/walgreen-pharmacy-customer-scores-1-4m-privacy-verdict.

236. Oullette, *supra* note 233.

237. *Id.* (HIPAA violations are typically reported directly to the U.S. Department of Health and Human Services, which then decides whether or not to investigate claims of privacy breach).

238. *Id.*

239. *Id.*

240. Scurria, *supra* note 235.

241. *Id.*

Dreyer also ruled that Indiana state law "could support a tort claim arising from public disclosure of private facts – even if the disclosure in question involved only one other person."[243]

Despite evidence that privacy breaches of PHI occur frequently,[244] the Walgreens verdict is only one of two jury verdicts[245] awarded against healthcare providers who have violated HIPAA Privacy Rules.[246] However, during the discovery proceedings, Walgreen refused to produce any documentation citing how frequently their employees had been disciplined for breaches similar to Audra Peterson's.[247] Furthermore, the case made no mention of any HHS monetary punishment for privacy breaches.[248]

B. Model Rules for HIPAA

Given the trend of PHI's movement toward cloud sharing, HHS can model future HIPAA rules after other Internet privacy regulations.[249] The Electronic Communications Privacy Act (ECPA)[250] aims to protect government access to e-mail and other computer records held by third

---

242. *See* Oullette, *supra* note 233 (HIPAA violations are typically reported directly to the U.S. Department of Health and Human Services who then decides whether or not to investigate claims of privacy breach).

243. Scurria, *supra* note 235.

244. *See generally HIPAA Enforcement Statistics*, CMS.GOV, http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/Enforcement/HIPAAEnforcementStatistics.html (last updated Aug. 22, 2013).

245. Josh Crank, *Walgreens Sued For Sharing Patient's Private Medical Info*, LAWYERS.COM (Aug. 12, 2013) http://blogs.lawyers.com/2013/08/salgreens-shared-medical-record/ (Abigail Hinchy's attorney Neal F. Eggeson won a similar jury verdict where plaintiff's unredacted medical records were forwarded to a collection agency).

246. Oullette, *supra* note 233 (comment by Abigail Hinchy's attorney Neal F. Eggeson whose research then showed that only two jury verdicts existed).

247. *Id.*

248. *See generally id.*

249. *See State Laws Related to Internet Privacy*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 23, 2014) http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx (examples of various state laws focused on Internet privacy).

250. *See generally*, Electronic Communication Privacy Act 18 U.S.C. §§2510–2522 (2012).

parties.[251] Although there is controversy surrounding ECPA's efficacy,[252] the Act addresses concerns identical to concerns about cloud storage and PHI privacy.[253] For example, ECPA's broad definition of third parties makes it difficult to determine which acts and communications are actually protected by ECPA.[254] ECPA also addresses factors that impact PHI and cloud storage such as whether or not PHI in the cloud is classified as storage or communication and how to assess the quality of a provider's terms of services.[255]

In response to Internet privacy concerns, the Consumer Privacy Bill of Rights (hereinafter "the Bill") was created to establish a "comprehensive statement of the rights consumers should expect and the obligation to which companies handling personal data should commit."[256] The Bill defines personal data as "any data, including aggregations of data, that is linkable to a specific individual . . . and may include data that is linked to a specific computer or other device."[257] Most significantly, the Bill acknowledges that enforcement of privacy rights needs to be a multi-stakeholder process that involves other government agencies such as the Federal Trade Commission.[258]

Additionally, HHS should collaborate with private cloud storage providers to understand how the Rules should be addressed. Although the process for promulgating the Rules allowed for public comments, it is

---

251. S. Subashini & V. Kavitha, *A Survey on Security Issues in Service Delivery Models of Cloud Computing*, 34 J. NETWORK & COMPUTER APPLICATIONS 1, 6 (2011).

252. *See generally* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective On The Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1561-64 (2004).

253. *See generally* Subashini & Kavitha, *supra* note 251, at 2.

254. *See id.* at 6.

255. *See id.*

256. Office of the Press Secretary, *Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights*, THE WHITE HOUSE (Feb. 23, 2012), http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b.

257. *Id.*

258. Press Release, The White House Office of the Press Secretary, *Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights*, THE WHITE HOUSE, (Feb. 23, 2012), http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b.

unclear who submitted these comments and whether or not experts in the field of cloud computing were consulted.[259] For example, the Cloud Security Alliance is currently a collaborative forum dedicated to establishing standards for cloud storage providers.[260] Additionally, the Open Web Application Security Project maintains an updated list of the top threats to cloud storage.[261] The Open Grid Forum also publishes documents and papers with security and infrastructural specifications for cloud computing developers and researchers.[262] The European Union (EU) is currently addressing privacy and cloud storage concerns through a Network Security Policy that standardizes how countries respond to a cyber-attack or breach of privacy.[263] For example, EU Directive 95/46 protects PHI by prohibiting transfers to countries within the EU that do not meet the set standard of protection.[264] Additionally, transfer of PHI to countries outside of the EU requires the owner's consent.[265]

C. Conclusions and Recommendations

While expanding the scope of who is covered by HIPAA is a step in the right direction, further steps are needed to adequately protect the intersection of PHI with the technology of cloud storage. Additionally, given the increasing autonomy technology provides, the legal remedies for HIPAA privacy violations need to match the pace of technological growth.

---

259. *See generally*, Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules, 78 Fed. Reg. 5566, 5566 (proposed Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 and 164) (public comments were submitted for all proposed rules and responses to comments were submitted).

260. *See generally*, CLOUD SECURITY ALLIANCE, https://cloudsecurityalliance.org/ (last visited Feb. 21, 2014); *see also* Subashini & Kavitha, *supra* note 251 at 9.

261. *See generally*, THE OPEN WEB APPLICATION SECURITY PROJECT (OWASP), https://www.owasp.org/index.php/Main_Page (last visited Feb. 9, 2014); *see also* Subashini & Kavitha, *supra* note 251 at 9.

262. *See generally*, OPEN GRID FORUM, http://www.ogf.org/dokuwiki/doku.php (last visited Feb. 19, 2014); *see also* Subashini & Kavitha, *supra* note 251, at 9.

263. *Action 28: Reinforced Network and Information Security Policy*, EUROPEAN COMMISSION (Dec. 16, 2011), http://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-28-reinforced-network-and-information-security-policy.

264. Chunming Rong et al., *Beyond lightning: A Survey on Security Challenges in Cloud Computing*, 39 COMPUTERS & ELECTRICAL ENGINEERING 47, 49 (2013) (citing Article 25 and 26 of the European Union's Directive 95/46/EC).

265. *Id.*

First, HIPAA should be modeled after other successful privacy regulations[266] and utilize the research from pending and existing legislation.[267] Additionally, recommendations from private cloud storage companies should be incorporated into the Rules to establish technical guidelines for covered entities and business associates to follow.[268] Although the Rules aim to provide technological flexibility by remaining neutral on what technological protections cloud storage providers need to take, there are industry wide accepted standards that should be included in the Rules as a baseline level of protection for PHI.[269] At a bare minimum, PHI stored in the clouds should be encrypted, remain confidential, and owners should be able to clearly see who can access their PHI.[270]

Second, policymakers and legislators need to consider incorporating a private right of action under HIPAA. Although HHS has been delegated the authority to investigate HIPAA violations, the current model is ineffective at maximizing consumer protection. Even if a HIPAA violation is found, the victims of privacy breaches are rarely financially compensated.[271] Thus, even the most robust Rules that include all business entities, covered associates, and other health care providers do not benefit consumer privacy rights if consumers are not part of the equation.

Third, although consumers are allowed to waive certain privacy rights, HIPAA should prevent the ability for privacy to be waived in certain situations. Current requirements for waivers of privacy rights are too low and allow corporations to misleadingly encourage consumers to waive their

---

266. *See generally*, *State Laws Related to Internet Privacy*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 23, 2014), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

267. *See generally*, Adam Cohen, *Internet Privacy: A New Bill Finally Offers Protections*, TIME (Apr. 30, 2013), http://ideas.time.com/2013/04/30/internet-privacy-a-new-bill-finally-offers-protections/.

268. Wenjin Hu, Tao Yang, Jeanna N. Matthews, *The Good, the Bad and the Ugly of Consumer Cloud Storage*, 44 ACM SIGOPS OPERATING SYSTEMS REVIEW 3, 113 (July 2010).

269. *Id.* (listing recommendations such as compression of data before transferring PHI to a remote server, pre-processing tasks such as encryption, metadata creation, and metadata exchanges in incremental and parallel transfers, backing up contents regularly, and not relying on online backup services as a "whole system restore solution.").

270. Rong et al., *supra* note 264.

271. Ouellette, *supra* note 233 (citing Abigail Hinchy's attorney Neal F. Eggeson whose research then showed that only two jury verdicts existed).

privacy rights in exchange for a small reward.[272] To remedy this problem, HIPAA should either increase the requirements for a privacy waiver or create uniform policy that prevents any waiver of privacy rights in certain situations. HIPAA enforcement will only be meaningful if the regulations provide consumers with actual protection of privacy rights and a realistic and meaningful method to address any privacy violations.

272. David Lazarus, *CVS Thinks $50 Is Enough Reward for Giving Up Healthcare Privacy*, L.A. TIMES (Aug. 25, 2013, 5:54 PM), www.latimes.com/business/la-fi-lazarus-20130816,5,6795096,full.column#axzz2sgKSjlpA.